AO 106 (Rev. 01/09) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

District of Rhode Island

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
One ASUS laptop computer bearing serial number D5N0CV2633095198 and an 8 PNY gigabyte thumb drive

Case No. 1:17-MJ-411PAS

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that there is now concealed on the following person or property located in the ---------- District of Rhode Island *(identify the person or describe property to be searched and give its location):* one ASUS laptop computer bearing serial number D5N0CV2633095198 and an 8 gigabyte PNY thumb drive

The person or property to be searched, described above, is believed to conceal *(identify the person or describe the property to be seized)*: Evidence, fruits, contraband, and instrumentalities of receipt and distribution of child pornography, possession of child pornography, and access with intent to view child pornography as further described in Attachment B, incorporated by reference as if fully set forth.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of 18 U.S.C. § 2252 & 2252A, and the application is based on these facts:

See attached affidavit, incoprporated by reference

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of ___ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

James Richardson, Special Agent, HSI
Printed name and title

Sworn to before me and signed in my presence.

Date: Sept 7, 2017

Judge's signature

City and state: Providence, Rhode Island

Hon. Patricia A. Sullivan, U.S. Magistrate Judge
Printed name and title

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, James V. Richardson, a Special Agent (SA) with Homeland Security Investigations (HSI), being duly sworn, depose and state as follows:

INTRODUCTION

1. I have been employed as a Special Agent of the U.S. Department of Homeland Security, Homeland Security Investigations ("HSI") since 2009, and am currently assigned to the office of the Resident Agent in Charge (RAC), Providence, RI. While employed by HSI, I have investigated federal criminal violations related to high technology or cybercrime, child exploitation, and child pornography. I have gained experience through training at the Federal Law Enforcement Training Center in Brunswick, GA, and as a member of the Rhode Island Internet Crimes Against Children (ICAC) Task Force conducting these types of investigations. I have investigated child pornography cases and related sexual offenses on a full time basis since approximately January 2010. I have received training in the area of child pornography and child exploitation, and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media including computer media. I have conducted and assisted in conducting numerous investigations into the violation of both state and federal laws relating to the possession, receipt, transportation, distribution, and production of child pornography and obscene visual representations of the sexual abuse of children over the Internet. I have reviewed hundreds of images and videos of actual and suspected child pornography, child erotica, and obscene visual representations of the sexual abuse of children. Moreover, I am a federal law enforcement officer who is engaged in

enforcing the criminal laws, including 18 U.S.C. §§ 2252 and 2252A, and I am authorized by law to request a search warrant.

2. This affidavit is submitted in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant for the property specifically described in **Attachment A** of this Affidavit, to wit, one ASUS laptop computer bearing serial number D5N0CV2633095198 and an 8 PNY gigabyte thumb drive which was plugged into the laptop through the USB port and thumb drive seized via consent from a business called Northern Lights on August 21, 2017 for contraband and evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 2251, 2252, 2252A, and 2422, which items are more specifically described in **Attachment B** of this Affidavit.

3. On August 8, 2017, I applied for a search warrant to search the premises at 9 Grove Avenue, Floor 3, Westerly, RI, and any person located therein and submitted an affidavit in support. That affidavit is attached to this affidavit as Exhibit A and incorporated by reference and restated herein for purposes of this affidavit.

4. On August 9, 2017, the search warrant was executed by myself and other members of the Rhode Island Internet Crimes Against Children (ICAC) and HSI. The residence was occupied by Jonathan Breslin ("Breslin"). During the execution of the search warrant, several electronic media storage devices, including a laptop computer, a thumb drive, and an iPhone were seized pursuant to the search warrant and observed to contain child pornography.

5. Subsequent to executing the search warrant, but also on August 9, 2017, I applied for a criminal complaint charging Jonathan Breslin, (D.O.B. xx/xx/1985) with receiving and distributing child pornography in violation of 18 U.S.C. 2252(a)(2); possessing and accessing

with intent to view child pornography in violation of 18 U.S.C. 2252(a)(4); transfer of obscene material to a minor via interstate commerce in violation of 18 U.S.C. 1470; and attempted production of child pornography in violation of 18 U.S.C. § 2251(a) and (d). That affidavit is attached to this affidavit as Exhibit B and incorporated by reference and restated herein for purposes of this affidavit.

6. On August 16, 2017, Attorney Rebecca Cromwell contacted Assistant United States Attorney John McAdams, who is prosecuting this matter. Attorney Cromwell indicated that her family owned several stores, including Northern Lights, 771 Long Hill Road in Groton, Connecticut. Attorney Cromwell indicated that Northern Lights formerly employed Jonathan Breslin, but had terminated his employment in approximately March or April of 2017. Attorney Cromwell indicated that Breslin had abandoned a laptop computer at Northern Lights, and it was still there. Attorney Cromwell wanted to turn the laptop over to law enforcement.

7. On August 21, 2017, I went to Northern Lights and met with Matt Snydal, the manager of Northern Lights. I was voluntarily provided an ASUS laptop computer, bearing serial number D5N0CV2633095198 and an 8 gigabyte PNY thumb drive which was plugged into the laptop through the USB port. Snydal stated that after Breslin was arrested, Snydal told the owners of Northern Lights that Breslin had access to the laptop. The owners told Snydal that Northern Lights never owned or purchased any laptop computers for any of their stores, leading to Attorney Cromwell contacting the government. Mr. Snydal indicated that I would need to speak to Northern Lights' employee Dillon Kauffman to obtain more information about the abandonment of the laptop because Snydal started as a manager of the store after Breslin was terminated. Mr. Kaufmann was on vacation at the time. On August 25, 2017, I spoke with Mr.

Kauffmann via telephone. Mr. Kaufmann stated that a former manager, Matt LNU (not Snydal), and Breslin used the laptop. The former manager only used the laptop to post Northern Lights information to Instagram. Breslin also used the laptop for unknown purposes. After Matt LNU stopped working at Northern Lights, only Breslin used the laptop, and Breslin was the only person who knew the password. The laptop had not been used since Breslin was fired. *

8. Based on my training and experience, I know that individuals who view and possess child pornography frequently maintain child pornography on various electronic media storage devices over which they exercise dominion and control. I also know that individuals who view and possess child pornography frequently access websites where they can view and download child pornography using any device on which they have access. In this instance, Breslin had child pornography files on multiple electronic media storage devices. The thumb drive which was seized from Breslin's residence, which contained child pornography files, and which Breslin admitted contained child pornography files, was the same size and brand (8 gigabyte PNY) as the thumb drive attached to the laptop provided by Northern Lights. Accordingly, there is probable cause to believe there will be evidence of crimes involving the possession and receipt on the laptop computer and thumb drive voluntary provided by Northern Lights.

CONCLUSION

9. Based on the foregoing, there is probable cause to believe that the federal criminal statutes cited herein have been violated, and that the contraband, property, evidence, fruits and instrumentalities of these offenses, more fully described in Attachment B, are located at the locations described in Attachment A. I respectfully request that this Court issue a search warrant for the locations described in Attachment A, authorizing the seizure and search of the items

* The seized property (laptop and thumb drive) are currently located in the RI State Police evidence room in Warwick, RI.

described in Attachment B.

10. I am aware that the recovery of data by a computer forensic analyst takes significant time; much the way recovery of narcotics must later be forensically evaluated in a lab, digital evidence will also undergo a similar process. For this reason, the "return" inventory will contain a list of only the tangible items, to wit, the laptop and the thumb drive. Unless otherwise ordered by the Court, the return will not include evidence later examined by a forensic analyst.

James V. Richardson
Special Agent
Homeland Security Investigations

Sworn and subscribed before me this 7th day of September, 2017.

HON. PATRICIA A. SULLIVAN
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

DESCRIPTION OF LOCATIONS TO BE SEARCHED

One ASUS laptop computer bearing serial number D5N0CV2633095198 and an 8 gigabyte PNY thumb drive connected to it via USB port.

ATTACHMENT B

ITEMS TO BE SEIZED

The following materials, which constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use or which is or has been used as the means of committing a criminal offense, namely violations of Title 18, United States Code, Sections 2252, 2252A and 2422:

1. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):
    a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
    b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
    c. evidence of the lack of such malicious software;
    d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to the crime(s) under investigation and to the computer user;

e. evidence indicating the computer user's knowledge and/or intent as it relates to the crime(s) under investigation;

f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

g. evidence of programs (and associated data) that are designed to eliminate data from the COMPUTER;

h. evidence of the times the COMPUTER was used;

i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

k. records of or information about Internet Protocol addresses used by the COMPUTER;

l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses; and

m. contextual information necessary to understand the evidence described in this attachment.

2. Child pornography and child erotica.

EXHIBIT A

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, James V. Richardson, a Special Agent (SA) with Homeland Security Investigations (HSI), being duly sworn, depose and state as follows:

INTRODUCTION

1. I am a Special Agent with United States Department of Homeland Security (DHS), Immigrations and Customs Enforcement, Homeland Security Investigations (HSI), and am assigned to the office of the Special Agent in Charge, Providence, RI. I have been an agent of HSI since 2009. As part of my duties, I am authorized to investigate violations of the laws of the United States, including criminal violations relating to child exploitation, child pornography, coercion and enticement, and transportation of minors, including but not limited to, violations of 18 U.S.C. §§ 2422, 2251, 2252, and 2252A. I have received training in the investigation of child pornography, child exploitation, and transportation of minors, and have had the opportunity to observe and review examples of child pornography (as defined in 18 U.S.C. § 2256).

2. This affidavit is submitted in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant for the locations specifically described in **Attachment A** of this Affidavit, including the entire property located at 9 Grove Avenue, Floor 3, Westerly, RI 02891 (the "SUBJECT PREMISES"), the content of electronic storage devices located therein, any person located at the SUBJECT PREMISES, for contraband and evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 2251, 2252, 2252A, and 2422, which items are more specifically described in **Attachment B** of this Affidavit.

3. The statements in this affidavit are based in part on information provided by HSI agents in Ottawa, Canada, and on my investigation of this matter. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that contraband and evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 2252(a)(2) and (b)(1) (distribution of a visual depiction of a minor engaged in sexually explicit conduct); 18 U.S.C. §§ 2252A(a)(2)(A) and (b)(1) (distribution of child pornography); 18 U.S.C. §§ 2252(a)(4)(B) and (b)(2) (possession of and access with intent to view a visual depiction of a minor engaged in sexually explicit conduct); 18 U.S.C. §§ 2252A(a)(5)(B) and (b)(2) (possession of and access with intent to view child pornography); and 18 U.S.C. § 2422(b) (use of means of interstate or foreign commerce to persuade, entice, or coerce a minor to engage in explicit sexual activity) are presently located at the SUBJECT PREMISES.

STATUTORY AUTHORITY

4. As noted above, this investigation concerns alleged violations of the following:

a. Title 18, United States Code, Sections 2252(a)(2) and (b)(1) prohibit any person from knowingly receiving or distributing, or attempting or conspiring to receive or distribute, any visual depiction using any means or facility of interstate or foreign commerce, or that has been mailed or shipped or transported in or affecting interstate or foreign commerce, or which contains materials which have been mailed or so shipped or transported, by any means including by computer, or knowingly reproducing any visual depiction for distribution using any means or facility of interstate or foreign commerce,

or in or affecting interstate or foreign commerce or through the mails, if the production of such visual depiction involved the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct.

b. Title 18, United States Code, Sections 2252A(a)(2)(A) and (b)(1) prohibit a person from knowingly receiving or distributing, or attempting or conspiring to receive or distribute, any child pornography or any material that contains child pornography, as defined in 18 U.S.C. § 2256(8), that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

c. Title 18, United States Code, Sections 2252(a)(4)(B) and (b)(2) prohibit any person from knowingly possessing or accessing with the intent to view, or attempting or conspiring to possess or access with the intent to view, 1 or more books, magazines, periodicals, films, video tapes, or other matter which contain any visual depiction that has been mailed, or has been shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, or which was produced using materials which have been mailed or so shipped or transported, by any means including by computer, if the production of such visual depiction involved the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct.

d. Title 18, United States Code, Sections 2252A(a)(5)(B) and (b)(2) prohibit a person from knowingly possessing or knowingly accessing with intent to view, or attempting or conspiring to do so, any material that contains an image of child

pornography, as defined in 18 U.S.C. § 2256(8), that has been mailed, or shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, by any means, including by computer, or that was produced using materials that have been mailed or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

e. Title 18, United States Code, Section 2422(b) prohibits any person from using a means of interstate or foreign commerce to persuade, induce, entice, or coerce any person under the age of eighteen to engage in sexual activity for which any person can be charged with an offense, or attempting to do so.

DEFINITIONS

5. The following definitions apply to this Affidavit and Attachment B:

a. "Chat," as used herein, refers to any kind of text communication over the Internet that is transmitted in real-time from sender to receiver. Chat messages are generally short in order to enable other participants to respond quickly and in a format that resembles an oral conversation. This feature distinguishes chatting from other text-based online communications such as Internet forums and email.

b. "Chat room," as used herein, refers to the ability of individuals to meet in one location on the Internet in order to communicate electronically in real-time to other individuals. Individuals may also have the ability to transmit electronic files to other individuals within the chat room.

c. "Child erotica," as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily obscene or do not necessarily depict minors engaging in sexually explicit conduct.

d. "Child pornography," as defined in 18 U.S.C. § 2256(8), is any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image of picture, whether made or produced by electronic, mechanical or other means, of sexually explicit conduct, where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

e. "Computer," as used herein, refers to "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device" and includes smartphones, and mobile phones and devices. *See* 18 U.S.C. § 1030(e)(1).

f. "Computer hardware," as used herein, consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes,

and other memory storage devices); peripheral input/output devices (including keyboards, printers, video display monitors, and related communications devices such as cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including physical keys and locks).

g. "Computer passwords and data security devices," as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates what might be termed a digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

h. "Hashtag," as used herein, refers to a word or phrase preceded by a hash or pound sign (#), which is used to identify messages or groups on a specific topic.

i. "Internet Protocol address" or "IP address," as used herein, refers to a unique number used by a computer or other digital device to access the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer or device accessing the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer or device may be directed properly from its source to its destination. Most Internet Service

Providers (ISPs) control a range of IP addresses. IP addresses can be "dynamic," meaning that the ISP assigns a different unique number to a computer or device every time it accesses the Internet. IP addresses might also be "static," if an ISP assigns a user's computer a particular IP address that is used each time the computer accesses the Internet. ISPs typically maintain logs of the subscribers to whom IP addresses are assigned on particular dates and times.

j. "Internet Service Providers" ("ISPs"), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment.

k. The "Internet" is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

l. "Minor," as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.

m. "Mobile applications," as used herein, are small, specialized programs downloaded onto mobile devices that enable users to perform a variety of functions, including engaging in online chat, reading a book, or playing a game.

n. "Records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.

o. "Remote Computing Service" ("RCS"), as defined in 18 U.S.C. § 2711(2), is the provision to the public of computer storage or processing services by means of an electronic communications system.

p. "Sexually explicit conduct," as defined in 18 U.S.C. § 2256(2), means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person.

q. A "storage medium" is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, thumb drives, and other magnetic or optical media.

r. "Visual depiction," as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

PROBABLE CAUSE

6. Canadian law enforcement officers have reported to HSI that on March 22, 2016, an officer with the Saskatchewan Police Service (SPS) in Saskatchewan, Canada, arrested an

individual (hereinafter "John Doe") for parole violations.[1] Pursuant to the arrest, SPS seized John Doe's iPhone. John Doe told SPS that he had been using an online mobile chat application to download and distribute child pornography images and videos to a network of other users of the mobile chat application. He provided SPS his username and login information for the application and gave SPS consent to take over and use his account to conduct investigations and gather evidence. This chat application is hereinafter referred to as "Application A."[2] HSI was not involved with the user's arrest.

7. "Application A" is designed for mobile chatting or messaging. To use this application, a user downloads the application to a mobile phone or other mobile device via a service such as Google Play Store, Apple iTunes, or another similar provider. Once downloaded and installed, the user is prompted to create an account and username. The user also has a display name, which is what other users see when transmitting messages back and forth. Once the user has created an account, the user is able to locate other users via a search feature, and the two parties can then send each other messages, images, and videos.

8. "Application A" users are also able to create chat groups, of up to 50 people, to communicate in a group setting and exchange images and videos. These groups are administered

---

[1] John Doe's true name is known to law enforcement. This investigation remains active and disclosure of Doe's true name would potentially alert investigative suspects to the fact that law enforcement action is being taken, thereby provoking suspects to notify other users of law enforcement action, flee, and/or destroy evidence.

[2] The actual name of "Application A" is known to law enforcement. This chat application remains active and disclosure of the name of the application would potentially alert its users to the fact that law enforcement action is being taken against users of the application, thereby provoking users to notify other users of law enforcement action, flee, and/or destroy evidence. Accordingly, to protect the confidentiality and integrity of the ongoing investigation involved in this matter, specific names and other identifying factors have been replaced with generic terms and the application will be identified herein as "Application A."

by the group creator who has the authority to remove and ban other users from the created group. Once the group is created, "Application A" users have the option of sharing a link to the group that includes all of their contacts or any other user. These groups are frequently created with a "hashtag" that is easily identifiable or searchable by keyword.

9. SPS was able to log in and secure John Doe's "Application A" account. In reviewing the chat conversations held with John Doe's account, SPS was able to identify 72 unique "Application A" users who had shared at least one image or video of child pornography with John Doe directly, or who had posted child pornography in one of the "Application A" groups to which John Doe belonged, and six "Application A" users who had posted a message between or commented on child pornography images or videos. Many of the groups to which John Doe belonged had names that included terms that your affiant knows through training and experience to be suggestive of child pornography.

10. SPS logged all of the information regarding the messages and saved all of the images and videos of child pornography shared with John Doe's account. SPS sent preservation requests to "Application A" regarding all 78 accounts referenced in the previous paragraph between April 20 and April 30, 2016. SPS transmitted to HSI the information logged and saved from the review of John Doe's "Application A" account.

11. On June 28, 2016, a Production Order was issued by a Provincial Court Judge in Saskatchewan, Canada, ordering "Application A" to produce user information and saved content regarding these 78 accounts. On September 15, 2016, SPS received the requested results from "Application A." The information received from "Application A," including the Certification of

Records provided by "Application A," was transmitted to HSI, along with a copy of the Production Order issued by the Provincial Court Judge.

12. The results provided by "Application A" included, among other things, additional images and videos of child pornography recently shared by the 78 accounts. This included both child pornography shared with John Doe and child pornography shared with other individuals and groups not related to John Doe's account. Additional Production Orders were served on "Application A" for information regarding the "Application A" accounts who shared child pornography with the originally investigated 78 accounts, leading to the identification of additional "Application A" accounts beyond the 78 accounts that shared child pornography with John Doe.

13. Your affiant has reviewed the information received from "Application A." A review of that information shows that April 2, 2016 an "Application A" user with the account name "bluegreen19" used "Application A" to share a video of child pornography. Specifically, the video shared by "bluegreen19" included the following:

a. **File name:** 1459568709575-cc4ab178-3a9b-480d-a859-49e40a8b3fd1.mp4

Description: a video, approximately 24 seconds in length, of an adult female inserting a sexual device into a nude prepubescent female's anus.

14. The information provided by "Application A" included IP addresses used by the target account. Specifically, IP address 100.40.20.91 was used by "bluegreen19" on February 25, 2017 at 04:47:17 UTC. A query of the American Registry for Internet Numbers ("ARIN")

online database revealed that IP address 100.40.20.91 was registered to Verizon Internet Services, Inc. ("Verizon").

15. On June 9, 2017, a U.S. Department of Homeland Security summons was issued to Verizon in regard to the IP address described in Paragraph 12. A review of the results obtained on June 23, 2017 identified the following account holder and address, which is the address of the SUBJECT PREMISES:

IP Address:	100.40.20.91
Start time:	2016-08-17 @ 05:08:11Z
Stop time:	2017-04-26 @ 04:32:11Z
Duration:	251d 23h 24min 0s
Customer ID:	154084724
Customer name:	Jonathan Breslin
Account address:	9 Grove Av FLR 3 WSTY, RI 02891
User ID:	vze1el1ow
User Name:	jbreslin710

16. A check of publicly available databases also revealed that Jonathan BRESLIN resides at the SUBJECT PREMISES.

17. A check with the Rhode Island State Police (RISP) Fusion Center on or about July 3, 2017, revealed that an individual named Jonathan BRESLIN with a date of birth of

(XX/XX/1985) has a RI driver's license with a previous address listed. The check also revealed that BRESLIN does not have any vehicles registered in his name.

18. On or about July 11, 2017, representatives of the U.S. Postal Service stated that Jonathan BRESLIN is currently receiving mail at the SUBJECT PREMISES.

19. Surveillance of the SUBJECT PREMISES on or about July 7, 2017 revealed that the number "9" is clearly marked on the front door of the house.

20. A search of a public records database that provides names, dates of birth, addresses, associates, telephone numbers, email addresses, etc., was conducted for Jonathan BRESLIN. These public records indicated that BRESLIN's current address is 9 Grove Avenue, Apartment 3, Westerly, RI 02891. The records also indicated that an email address BRESLIN provided to "Application A" (rainshadow39@gmail.com) is also affiliated with an Amazon account in the name of Jonathan BRESLIN.

21. A check of open source information from the Internet regarding BRESLIN revealed that BRESLIN, using the SUBJECT PREMISES address, filed corporation paperwork in the state of Connecticut on January 17, 2017 for a company named Poquonnock Group, LLC. The website also revealed that the company dissolved in June of 2017.

22. On July 28, 2017, I served an administrative subpoena on Application A for subscriber information for the username "Bluegreen19." On July 31, 2017, Application A responded with updated IP address information for "Bluegreen19." Specifically, IP address 108.34.203.193 was used by "bluegreen19" on July 2, 2017 at 01:11:53 UTC and July 29, 2017 at 13:25:25 UTC. A query of the American Registry for Internet Numbers ("ARIN") online

database revealed that IP address 108.34.203.193 was registered to Verizon Internet Services, Inc. ("Verizon").

23. On July 31, 2017, a U.S. Department of Homeland Security summons was issued to Verizon in regard to the IP address described in Paragraph 22. A review of the results obtained on August 7, 2017 identified the following account holder and address, which is the address of the SUBJECT PREMISES:

IP Address: 108.34.203.193

Customer ID: 154084724

Customer name: Jonathan Breslin

Account address: 9 Grove Av
FLR 3
WSTY, RI 02891

User ID: vze1el1ow

User Name: jbreslin710

24. On August 1, 2017, acting in an undercover capacity, your affiant sent an unsolicited "chat" message to the username "Bluegreen19" via "Application A." "Bluegreen19" responded shortly thereafter. The initial unsolicited chat and response are excerpted as follows:

UCA (undercover affiant) – I lost all my good stuff!

BLUEGREEN19 – Mr discreet lol

UCA – You like that? Lol

BLUEGREEN19 – Almost too discreet lol

UCA – My computer crashed and I lost everything

BLUEGREEN19 – Where do I know you from?

UCA – I saved your contact after we talked in a "group" a while back. I only save the ones I trust.

BLUEGREEN19 – Gottttcha

25. "Bluegreen19" provided some technical advice regarding recovering lost data, then the following exchange occurred in which "Bluegreen19" suggested using another social media application, "Application B" to obtain child pornography and child erotica:

UCA – Can you hook a brother up? lol

BLUEGREEN19 – Did u ever check out [Application B]?

BLUEGREEN19 – I panicked and deleted everything lol

UCA – It may have been in my favorites

BLUEGREEN19 – I only have candids of girls eating ice cream next door lol

UCA – Wh did you panic?

BLUEGREEN19 – Gf found out I cheated on her, thought she was gonna DIG through my phone

UCA – Oh shit! That sucks!

BLUEGREEN19 – U don't even know…

UCA – You sent me some good shit a while back! That's why I saved you! Lol

BLUEGREEN19 – [Application B]

BLUEGREEN19 – Get. That. Shit. Lol

26. Application B is a mobile application that provides users a platform to post videos of themselves and share them with friends or the world. Application B also contains a feature which allows the user to stream themselves live. Within Application B, users can post comments to a broadcaster's performance and send "likes" to the performers they enjoy. Users create a

username and password, and can follow other users. Application B's terms of service require that users be at least 13 years old to use the platform and its guidelines state that users should not post sexually explicit or nude videos or images.

27. "Bluegreen19" described viewing videos of children engaged in sexually explicit activity notwithstanding Application B's terms of service:

UCA – It's an app? What's kind of shit is on there?

BLUEGREEN19 – I got banned for comments..u can't use keywords but those girls do CRAZY shit with HD cams

BLUEGREEN19 – Its supposed to be a sing along lip sync music video thing

BLUEGREEN19 – But girls can go live

UCA – Nice! How old?

BLUEGREEN19 – Younnnggggg lol

UCA – And they do more than sing? Lol

BLUEGREEN19 – Omg yes

BLUEGREEN19 – I watched what had to be an 8yo stick a mini toy bowling pin(the top part) up her ass, pull it out and suck on it

BLUEGREEN19 – Girls in the tub pissing into their mouths

BLUEGREEN19 – So many close up orgasms

BLUEGREEN19 – I really need to get that shit back…

UCA – Can't you just sign up under a different name?

BLUEGREEN19 – Girls TRYING to stick things in their pussies and saying ow

BLUEGREEN19 – Yeah totally

BLUEGREEN19 – I get paranoid and try to stay away but goddamn

BLUEGREEN19 – The shit I've seen

28. Bluegreen19 then stated that he convinced some minor females that he found on Application B to communicate with him on Application A and coerced at least one minor female to engage in sexually explicit activity:

BLUEGREEN19 – Got a few of them to hit me up on [Application A]

BLUEGREEN19 – Oh shit ill give u her name

BLUEGREEN19 – Just share what u get lol

UCA – Absolutely! I'm so hard up for that shit right now!

BLUEGREEN19 – [username redacted by your affiant]

UCA – And how old is she?

BLUEGREEN19 – She won't talk to me anymore lol

UCA – Why?

BLUEGREEN19 – She said 13 but not older than ten

UCA – Wow! And she did the shit you told her to do?

BLUEGREEN19 – She showed her pussy and face in the same pic

BLUEGREEN19 – Sexy fucking glasses

BLUEGREEN19 – Bald n wet

29. Your affiant reviewed the Application B account of the username identified above by "Bluegreen19" and observed a video of a minor female, approximately 8 to 10 years old, lipsyncing a pop song and licking her lips in a sexually suggestive manner.

30. "Bluegreen19" also described showing pornographic material to minors:

BLUEGREEN19 – I showed these 2 little girls a rough gangbang vid and they were like "stop it! They're being mean to the pretty lady!" I had to explain that she likes it

31. Your affiant asked "Bluegreen19" about groups on Application A:

UCA – Any good [Application A] groups groups lately? Every good one I find is full! So frustrating!

BLUEGREEN19 – Lol

BLUEGREEN19 – I haven't been in one in ages

BLUEGREEN19 – I only have non nude candids

UCA – Well I know you had some good shit back then because like I said I only save the ones I like and trust! Lol

32. At this point, "Bluegreen19" sent me three image of a fully clothed minor female. It appears that the pictures were taken out of the window of a car.

33. "Bluegreen19" subsequently sent a link to a video on Application B. The video is child erotica of a minor female in a bikini dancing in a seductive manner. The girl then turns around and the bathing suit bottom is pulled up into the crack of her bottom. "Bluegreen19" then sent another link to video on Application B of a minor female in underwear or pajamas dancing. The girl's bottoms are pulled up showing the outline of her vagina.

34. On August 4, 2017, "Bluegreen19" sent me a chat via Application A in which he described wanting to molest his girlfriend's 6 or 7 year old niece:

BLUEGREEN19 – Had a dream last night I was jerking off over my gfs nieces sleeping face, was so real

BLUEGREEN19 – Any headway in [Application B]?

UCA – Not yet. I guess networking takes some time! I tried the hard drive thing to recover my stash and it didn't work

BLUEGREEN19 – There's def ways to recover them, might have to spend some money on recovery software

BLUEGREEN19 – I wish I didn't delete all my shit…

BLUEGREEN19 – Had a ton of vids of little girls getting flashed with big dick, loved the reactions

UCA – Have to build the stash back up lol

BLUEGREEN19 – So paranoid these days lol fuckin sucks

UCA – Things will blow over with the gf

BLUEGREEN19 – I want to get the niece to sleep over fuckin bad lol

BLUEGREEN19 – Want her *

BLUEGREEN19 – It's a loft style apartment so it's one giant room, would be so easy to jerk it right over her sleeping face and cum on her pillow

BLUEGREEN19 – After my gf falls asleep of course

BLUEGREEN19 – I thought maybe I could cum on her lips and could say she was drooling if she woke up…But that's risky business lol

UCA – Especially if the gf is sleeping in the same room!

BLUEGREEN19 – Fuck yes!

BLUEGREEN19 – I want her to fall asleep on my lap so I can rub my dick on her little mouth without a lot of moving around

BLUEGREEN19 – Trying to have a star wars night with her (so the gf leaves)

UCA – How old?

BLUEGREEN19 – I'd go in the next room and shoot the biggest load into a bowl of ice cream and cover it with chocolate syrup and whipped cream and only put one small scoop so when she asks for more I can tell her to lick the bowl clean first

BLUEGREEN19 –6or7now

BLUEGREEN19 – What would you do?

UCA – I think you are braver than I am lol

BLUEGREEN19 – Lol

BLUEGREEN19 – It would be hot if she was just pretending to sleep

UCA – You think she'd sleep thru it?

BLUEGREEN19 – My gf?

BLUEGREEN19 – Or getting cum shot on her lips?

35. "Bluegreen19" then described possibly drugging the minor female in order to molest her:

BLUEGREEN19 – I'd like to get her tuckered out from playing in the snow or something, maybe crush up a tylenol pm on that ice cream or something

BLUEGREEN19 – Some kids when they pass out u can pick them up and put them in bed and they are OUT

BLUEGREEN19 – I think you'd have a shot of they were that out

UCA – Have you ever done anything like that before? So hot!

BLUEGREEN19 – I haven't but I think about it all the time lol

36. At this point, "bluegreen19" sends a link to a video on Application B. The video is of a minor female in a bikini dancing on what appears to be beach. The girl pulls on the bikini top and the bikini bottoms show the outline of her vagina.

37. In addition, "Bluegreen19" a link to a video of post-pubescent pornography on Application B, specifically a close up video of a post-pubescent female urinating. It is unclear whether the video is of an adult or a post-pubescent minor.

38. On August 8, 2017, "Bluegreen19" sent me a "chat" message via Application A in which he again referred to possible molesting his girlfriend's niece:

BLUEGREEN19: Lol I gotta bring up movie night without sounding fucking weird

UCA: Your gf would think its weird if you wanted to do a movie night?

BLUEGREEN19: No either she or the kid brought it up already, just gotta figure out how to work it out without being weird

BLUEGREEN19: Maybe I can take her swimming and get her to take a shower after

39. At this point, "Bluegreen19" sent me a link to a video on Application B featuring a minor female, approximately 7 or 8 years old years old, wearing a bikini top and panty underwear, dancing.

BLUEGREEN19: This girls fuckin body…i just wanna bury my face in that ass

BLUEGREEN19: I would drug the shit out of that girl if I had half a chance

BACKGROUND ON CHILD PORNOGRAPHY, COMPUTERS, AND THE INTERNET

40. I have had both training and experience in the investigation of computer-related crimes. Based on my training, experience, and knowledge, I know the following:

a. Computers and digital technology are the primary way in which individuals interested in child pornography interact with each other. Computers basically serve four functions in connection with child pornography: production, communication, distribution, and storage.

b. Digital cameras and smartphones with cameras save photographs or videos as a digital file that can be directly transferred to a computer by connecting the camera or smartphone to the computer, using a cable or via wireless connections such as "WiFi" or "Bluetooth." Photos and videos taken on a digital camera or smartphone may be stored on a removable memory card in the camera or smartphone. These memory cards are often large enough to store thousands of high-resolution photographs or videos.

c. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Mobile devices such as smartphones and tablet computers may also connect to other computers via wireless connections. Electronic contact can be made to literally millions of computers around the world. Child pornography can therefore be easily, inexpensively and anonymously (through electronic communications) produced, distributed, and received by anyone with access to a computer or smartphone.

d. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. Electronic storage media of various

types – to include computer hard drives, external hard drives, CDs, DVDs, and "thumb," "jump," or "flash" drives, which are very small devices which are plugged into a port on the computer – can store thousands of images or videos at very high resolution. It is extremely easy for an individual to take a photo or a video with a digital camera or camera-bearing smartphone, upload that photo or video to a computer, and then copy it (or any other files on the computer) to any one of those media storage devices. Some media storage devices can easily be concealed and carried on an individual's person. Smartphones and/or mobile phones are also often carried on an individual's person.

e. The Internet affords individuals several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

f. Individuals also use online resources to retrieve and store child pornography. Some online services allow a user to set up an account with a remote computing service that may provide e-mail services and/or electronic storage of computer files in any variety of formats. A user can set up an online storage account (sometimes referred to as "cloud" storage) from any computer or smartphone with access to the Internet. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer, smartphone or external media in most cases.

g. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional (*i.e.*, by saving an e-mail as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files).

Digital information can also be retained unintentionally such as the traces of the path of an electronic communication may be automatically stored in many places (*e.g.*, temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

41. As described above and in Attachment B, this application seeks permission to search for records that might be found at the SUBJECT PREMISES, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

42. I submit that if a computer or storage medium, including a smart phone, is found at the SUBJECT PREMISES, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file

on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

43. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the

purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium at the SUBJECT PREMISES because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information,

communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs,

may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

f. I know that when an individual uses a computer to obtain or access child pornography, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

44. Based upon my training and experience and information relayed to me by agents and others involved in the forensic examination of computers, I know that computer data can be stored on a variety of systems and storage devices, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact disks, magnetic tapes, memory cards,

memory chips, and online or offsite storage servers maintained by corporations, including but not limited to "cloud" storage. I also know that during the search of the premises it is not always possible to search computer equipment and storage devices for data for a number of reasons, including the following:

a. Searching computer systems is a highly technical process which requires specific expertise and specialized equipment. There are so many types of computer hardware and software in use today that it is impossible to bring to the search site all of the technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may also be necessary to consult with computer personnel who have specific expertise in the type of computer, software website, or operating system that is being searched;

b. Searching computer systems requires the use of precise, scientific procedures which are designed to maintain the integrity of the evidence and to recover "hidden," erased, compressed, encrypted, or password-protected data. Computer hardware and storage devices may contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Since computer data is particularly vulnerable to inadvertent or intentional modification or destruction, a controlled environment, such as a law enforcement laboratory, is essential to conducting a complete and accurate analysis of the equipment and storage devices from which the data will be extracted;

c. The volume of data stored on many computer systems and storage devices will typically be so large that it will be highly impractical to search for data during the execution of the physical search of the premises; and

d. Computer users can attempt to conceal data within computer equipment and storage devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension ".jpg" often are image files; however, a user can easily change the extension to ".txt" to conceal the image and make it appear that the file contains text. Computer users can also attempt to conceal data by using encryption, which means that a password or device, such as a "dongle" or "keycard," is necessary to decrypt the data into readable form. In addition, computer users can conceal data within another seemingly unrelated and innocuous file in a process called "steganography." For example, by using steganography a computer user can conceal text in an image file which cannot be viewed when the image file is opened. Therefore, a substantial amount of time is necessary to extract and sort through data that is concealed or encrypted to determine whether it is contraband, evidence, fruits, or instrumentalities of a crime.

45. Additionally, based upon my training and experience and information related to me by agents and others involved in the forensic examination of computers, I know that routers, modems, and network equipment used to connect computers to the Internet often provide valuable evidence of, and are instrumentalities of, a crime. This is equally true of so-called "wireless routers," which create localized networks that allow individuals to connect to the Internet wirelessly. Though wireless networks may be "secured" (in that they require an

individual to enter an alphanumeric key or password before gaining access to the network) or "unsecured" (in that an individual may access the wireless network without a key or password), wireless routers for both secured and unsecured wireless networks may yield significant evidence of, or serve as instrumentalities of, a crime—including, for example, serving as the instrument through which the perpetrator of the Internet-based crime connected to the Internet and, potentially, containing logging information regarding the time and date of a perpetrator's network activity as well as identifying information for the specific device(s) the perpetrator used to access the network. Moreover, I know that individuals who have set up either a secured or unsecured wireless network in their residence are often among the primary users of that wireless network.

46. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

CHARACTERISTICS COMMON TO INDIVIDUALS WHO ADVERTISE, TRANSPORT, DISTRIBUTE, RECEIVE, POSSESS, AND/OR ACCESS WITH INTENT TO VIEW CHILD PORNOGRAPHY

47. Based on my previous investigative experience related to child exploitation investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know there are certain characteristics common to individuals who distribute, receive, possess, and/or access with intent to view child pornography:

a. Such individuals may receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media, or from literature describing such activity.

b. Such individuals may collect sexually explicit or suggestive materials in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Such individuals almost always possess and maintain their hard copies of child pornographic material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. Individuals who have a sexual interest in children or images of children typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years.

d. As noted above, when your affiant, in an undercover capacity, asked "Bluegreen19" if he could "hook a brother up" (i.e., share child pornography), "Bluegreen19" stated that he "panicked and deleted everything" because his "Gf found out I cheated on her, thought she was gonna DIG through my phone." Based on my

training and experience, it is typical of individuals involved in child pornography to be initially reluctant to admit possessing child pornography or be willing to share such materials with other individuals on-line and to falsely and or inaccurately claim they deleted "all" of their child pornography collections. Often times such individuals maintain child pornography on a variety of different media and continue to keep child pornography even when some such materials are "deleted". This is particularly true of individuals, such as "Bluegreen19" who have distributed child pornography in the past.

e. Likewise, such individuals often maintain their child pornography images in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These child pornography images are often maintained for several years and are kept close by, usually at the possessor's residence, inside the possessor's vehicle, or, at times, on their person, to enable the individual to view the child pornography images, which are valued highly. Some of these individuals also have been found to download, view, and then delete child pornography on their computers or digital devices on a cyclical and repetitive basis.

f. Importantly, evidence of such activity, including deleted child pornography, often can be located on these individuals' computers and digital devices through the use of forensic tools. Indeed, the very nature of electronic storage means that evidence of the crime is often still discoverable for extended periods of time even after the individual "deleted" it.[3]

[3] *See United States v. Carroll*, 750 F.3d 700, 706 (7th Cir. 2014) (concluding that 5-year delay was not too long because "staleness inquiry must be grounded in an understanding of both the behavior of child pornography collectors

g. Such individuals also may correspond with and/or meet others to share information and materials, rarely destroy correspondence from other child pornography distributors/possessors, conceal such correspondence as they do their sexually explicit material, and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

h. Such individuals prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world. Thus, even if BRESLIN uses a portable device (such as a mobile phone) to access the internet and child pornography, it is more likely than not that evidence of this access will be found in his home, the SUBJECT PREMISES, as set forth in Attachment A.

REQUEST FOR SEALING OF WEBSITE/AFFIDAVIT

48. It is respectfully requested that this Court issue an order sealing, until further order of this Court, all papers submitted in support of this Application, including the Application, Affidavit, and Search Warrant, and the requisite inventory notice (with the exception of one copy of the warrant and the inventory notice that will be left at the SUBJECT PREMISES). Sealing is necessary because the items and information to be seized are relevant to an ongoing investigation and not all of the targets of this investigation will be searched at this time. Based upon my

---

and of modern technology"); *see also United States v. Seiver*, 692 F.3d 774 (7th Cir. 2012) (Posner, J.) (collecting cases, e.g., *United States v. Allen*, 625 F.3d 830, 843 (5th Cir. 2010); *United States v. Richardson*, 607 F.3d 357, 370–71 (4th Cir. 2010); *United States v. Lewis*, 605 F.3d 395, 402 (6th Cir. 2010).)

training and experience, I have learned that online criminals actively search for criminal affidavits and search warrants via the Internet, and disseminate them to other online criminals as they deem appropriate, *i.e.*, post them publicly online through forums. Premature disclosure of the contents of this Affidavit and related documents may have a significant and negative impact on this continuing investigation and may jeopardize its effectiveness by alerting potential targets to the existence and nature of the investigation, thereby giving them an opportunity to flee, or to destroy or tamper with evidence.

CONCLUSION

49. Based on the foregoing, there is probable cause to believe that the federal criminal statutes cited herein have been violated, and that the contraband, property, evidence, fruits and instrumentalities of these offenses, more fully described in Attachment B, are located at the locations described in Attachment A. I respectfully request that this Court issue a search warrant for the locations described in Attachment A, authorizing the seizure and search of the items described in Attachment B.

50. I am aware that the recovery of data by a computer forensic analyst takes significant time; much the way recovery of narcotics must later be forensically evaluated in a lab, digital evidence will also undergo a similar process. For this reason, the "return" inventory will contain a list of only the tangible items recovered from the premises. Unless otherwise ordered by the Court, the return will not include evidence later examined by a forensic analyst.

James V. Richardson
Special Agent
Homeland Security Investigations

Sworn and subscribed before me this 8 day of August, 2017.

HON. PATRICIA A. SULLIVAN
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

DESCRIPTION OF LOCATIONS TO BE SEARCHED

The entire property located at 9 Grove Avenue, Floor 3, Westerly, RI 02891, including the residential building, any outbuildings, and any appurtenances thereto (the SUBJECT PREMISES). The building is a three family, two and a half story building with yellow vinyl siding and white and green trim. The number "9" is clearly affixed to the front door of the building.

ATTACHMENT B

ITEMS TO BE SEIZED

The following materials, which constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use or which is or has been used as the means of committing a criminal offense, namely violations of Title 18, United States Code, Sections 2252, 2252A and 2422:

1. Computers or storage media, including smart phones, used as a means to commit the violations described above.
2. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):
    a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
    b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
    c. evidence of the lack of such malicious software;

d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to the crime(s) under investigation and to the computer user;

e. evidence indicating the computer user's knowledge and/or intent as it relates to the crime(s) under investigation;

f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

g. evidence of programs (and associated data) that are designed to eliminate data from the COMPUTER;

h. evidence of the times the COMPUTER was used;

i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

k. records of or information about Internet Protocol addresses used by the COMPUTER;

l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses; and

m. contextual information necessary to understand the evidence described in this attachment.

3. Routers, modems, and network equipment used to connect computers to the Internet.
4. Child pornography and child erotica.
5. Records, information, and items relating to violations of the statutes described above including:
    a. Records, information, and items relating to the occupancy or ownership of the SUBJECT PREMISES, 9 Grove Avenue, Floor 3, Westerly, RI 02891, including utility and telephone bills, mail envelopes, or addressed correspondence;
    b. Records, information, and items relating to the ownership or use of computer equipment found in the above residence, including sales receipts, bills for Internet access, and handwritten notes;
    c. Records and information relating to the identity or location of the persons suspected of violating the statutes described above;
    d. Records and information relating to the sexual exploitation of children, including correspondence and communications between users of "Application A" and "Application B";
    e. Records and information showing access to and/or use of "Application A" and "Application B"; and
    f. Records and information relating or pertaining to the identity of the person or persons using or associated with the "Application A" user "bluegreen19".

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing

or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact discs, magnetic tapes, memory cards, memory chips, and other magnetic or optical media.

EXHIBIT B

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A CRIMINAL COMPLAINT AND ARREST WARRANT

I, James V. Richardson, a Special Agent (SA) with Homeland Security Investigations, being duly sworn, hereby depose and state as follows:

INTRODUCTION

1. I have been employed as a Special Agent of the U.S. Department of Homeland Security, Homeland Security Investigations ("HSI") since 2009, and am currently assigned to the office of the Resident Agent in Charge (RAC), Providence, RI. While employed by HSI, I have investigated federal criminal violations related to high technology or cybercrime, child exploitation, and child pornography. I have gained experience through training at the Federal Law Enforcement Training Center in Brunswick, GA, and as a member of the Rhode Island Internet Crimes Against Children (ICAC) Task Force conducting these types of investigations. I have investigated child pornography cases and related sexual offenses on a full time basis since approximately January 2010. I have received training in the area of child pornography and child exploitation, and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media including computer media. I have conducted and assisted in conducting numerous investigations into the violation of both state and federal laws relating to the possession, receipt, transportation, distribution, and production of child pornography and obscene visual representations of the sexual abuse of children over the Internet. I have reviewed hundreds of images and videos of actual and suspected child pornography, child erotica, and obscene visual representations of the sexual abuse of children. Moreover, I am a federal law enforcement officer who is engaged in

enforcing the criminal laws, including 18 U.S.C. §§ 2252 and 2252A, and I am authorized by law to request a search warrant.

2. This affidavit is submitted in support of an application for a criminal complaint charging Jonathan Breslin, (D.O.B. xx/xx/1985) with receiving and distributing child pornography in violation of 18 U.S.C. 2252(a)(2); possessing and accessing with intent to view child pornography in violation of 18 U.S.C. 2252(a)(4); transfer of obscene material to a minor via interstate commerce in violation of 18 U.S.C. 1470; and attempted production of child pornography in violation of 18 U.S.C. § 2251(a) and (d).

3. On August 8, 2017, I applied for a search warrant to search the premises at 9 Grove Avenue, Floor 3, Westerly, RI, and any person located therein and submitted an affidavit in support. That affidavit is attached to this affidavit as Exhibit A and incorporated by reference and restated herein for purposes of this affidavit.

4. On August 9, 2017, the search warrant was executed by myself and other members of the Rhode Island Internet Crimes Against Children (ICAC) and HSI. The residence was occupied by Jonathan Breslin ("Breslin").

5. During the execution of the search warrant, ICAC Forensic Analyst Brittnee Morgan, who is trained in forensic computer examinations, conducted a preliminary review of an HP 2000 laptop computer bearing serial number 5CB1297H14. Analyst Morgan advised me that during her review she observed at least 12 video files containing child pornography on the laptop computer.

6. As described in paragraph 13 of Exhibit A, the username "Bluegreen19" distributed a video file containing child pornography on the social media application "Application A" on April 2, 2016.

7. Breslin's iPhone (describe) was reviewed by HSI Task Force Officer Detective Tim Grant of the Warwick Police Department. Detective Grant is trained in the forensic examination of mobile devices. Detective Grant specifically reviewed a chat on "Application A" between Breslin (as username "Bluegreen19) and observed the profile of a user who appeared to be a minor female. In the chat, Breslin asks the minor female how old she was when they first met, and the minor female responded "12." She further sated she is now either 14 or 15 years old. Detective Grant observed in the chat an exchange of pornographic photos between Breslin and the female. These photos included multiple photos sent by Breslin of an adult male's genitalia. In addition, in the chats, Breslin requests the minor to pose in certain ways. The female then sends back photos as requested, including at least one photo of her exposed breasts. Detective Grant estimates that, in his judgment, the female appears to be a minor, approximately 14 or 15 years.

8. Breslin was interviewed by myself and RISP Detective Adam Houston at the residence during the execution of the search warrant. Breslin was advised that he was not under arrest and also advised of his Miranda rights. Breslin signed the advice of rights form and agreed to voluntarily speak with us. Breslin then proceeded to state, among other things the following:

- Breslin admitted to receiving and possessing child pornography.
- Breslin admitted to being the username "Bluegreen19" on the social media application described in Exhibit A as "Application A."
- Breslin admitted to receiving and viewing child pornography on Application A.
- Breslin admitted to possessing child pornography on the HP 2000 laptop described above.

- Breslin also admitted to possessing child pornography on a thumb drive that was seized during the execution of the search warrant.
- Breslin estimated that the thumb drive contained between 100 and 200 child pornography files on the thumb drive.
- Breslin admitted using the social media application described as "Application B" in the Exhibit A.
- Breslin admitted using Application B to communicate with minor children.
- Breslin admitted sending photographs of his own genitalia via "Application A" to a user he believed was a minor female.

11. Based on the above, I believe there is probable cause to arrest Jonathon Breslin for knowingly receiving child pornography in violation of 18 U.S.C. 2252(a)(2); possessing and accessing with intent to view child pornography in violation of 18 U.S.C. 2252(a)(4); transfer of obscene material to a minor via interstate commerce in violation of 18 U.S.C. 1470; and attempted production of child pornography in violation of 18 U.S.C. §2251(a) and (d).

James V. Richardson
Special Agent
Homeland Security Investigations

Sworn and subscribed before me this 9th day of August, 2017.

HON. PATRICIA A. SULLIVAN
UNITED STATES MAGISTRATE JUDGE

Exhibit A

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, James V. Richardson, a Special Agent (SA) with Homeland Security Investigations (HSI), being duly sworn, depose and state as follows:

INTRODUCTION

1. I am a Special Agent with United States Department of Homeland Security (DHS), Immigrations and Customs Enforcement, Homeland Security Investigations (HSI), and am assigned to the office of the Special Agent in Charge, Providence, RI. I have been an agent of HSI since 2009. As part of my duties, I am authorized to investigate violations of the laws of the United States, including criminal violations relating to child exploitation, child pornography, coercion and enticement, and transportation of minors, including but not limited to, violations of 18 U.S.C. §§ 2422, 2251, 2252, and 2252A. I have received training in the investigation of child pornography, child exploitation, and transportation of minors, and have had the opportunity to observe and review examples of child pornography (as defined in 18 U.S.C. § 2256).

2. This affidavit is submitted in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant for the locations specifically described in **Attachment A** of this Affidavit, including the entire property located at 9 Grove Avenue, Floor 3, Westerly, RI 02891 (the "SUBJECT PREMISES"), the content of electronic storage devices located therein, any person located at the SUBJECT PREMISES, for contraband and evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 2251, 2252, 2252A, and 2422, which items are more specifically described in **Attachment B** of this Affidavit.

3. The statements in this affidavit are based in part on information provided by HSI agents in Ottawa, Canada, and on my investigation of this matter. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that contraband and evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 2252(a)(2) and (b)(1) (distribution of a visual depiction of a minor engaged in sexually explicit conduct); 18 U.S.C. §§ 2252A(a)(2)(A) and (b)(1) (distribution of child pornography); 18 U.S.C. §§ 2252(a)(4)(B) and (b)(2) (possession of and access with intent to view a visual depiction of a minor engaged in sexually explicit conduct); 18 U.S.C. §§ 2252A(a)(5)(B) and (b)(2) (possession of and access with intent to view child pornography); and 18 U.S.C. § 2422(b) (use of means of interstate or foreign commerce to persuade, entice, or coerce a minor to engage in explicit sexual activity) are presently located at the SUBJECT PREMISES.

STATUTORY AUTHORITY

4. As noted above, this investigation concerns alleged violations of the following:

a. Title 18, United States Code, Sections 2252(a)(2) and (b)(1) prohibit any person from knowingly receiving or distributing, or attempting or conspiring to receive or distribute, any visual depiction using any means or facility of interstate or foreign commerce, or that has been mailed or shipped or transported in or affecting interstate or foreign commerce, or which contains materials which have been mailed or so shipped or transported, by any means including by computer, or knowingly reproducing any visual depiction for distribution using any means or facility of interstate or foreign commerce,

or in or affecting interstate or foreign commerce or through the mails, if the production of such visual depiction involved the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct.

b. Title 18, United States Code, Sections 2252A(a)(2)(A) and (b)(1) prohibit a person from knowingly receiving or distributing, or attempting or conspiring to receive or distribute, any child pornography or any material that contains child pornography, as defined in 18 U.S.C. § 2256(8), that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

c. Title 18, United States Code, Sections 2252(a)(4)(B) and (b)(2) prohibit any person from knowingly possessing or accessing with the intent to view, or attempting or conspiring to possess or access with the intent to view, 1 or more books, magazines, periodicals, films, video tapes, or other matter which contain any visual depiction that has been mailed, or has been shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, or which was produced using materials which have been mailed or so shipped or transported, by any means including by computer, if the production of such visual depiction involved the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct.

d. Title 18, United States Code, Sections 2252A(a)(5)(B) and (b)(2) prohibit a person from knowingly possessing or knowingly accessing with intent to view, or attempting or conspiring to do so, any material that contains an image of child

pornography, as defined in 18 U.S.C. § 2256(8), that has been mailed, or shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, by any means, including by computer, or that was produced using materials that have been mailed or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

e. Title 18, United States Code, Section 2422(b) prohibits any person from using a means of interstate or foreign commerce to persuade, induce, entice, or coerce any person under the age of eighteen to engage in sexual activity for which any person can be charged with an offense, or attempting to do so.

DEFINITIONS

5. The following definitions apply to this Affidavit and Attachment B:

a. "Chat," as used herein, refers to any kind of text communication over the Internet that is transmitted in real-time from sender to receiver. Chat messages are generally short in order to enable other participants to respond quickly and in a format that resembles an oral conversation. This feature distinguishes chatting from other text-based online communications such as Internet forums and email.

b. "Chat room," as used herein, refers to the ability of individuals to meet in one location on the Internet in order to communicate electronically in real-time to other individuals. Individuals may also have the ability to transmit electronic files to other individuals within the chat room.

c. "Child erotica," as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily obscene or do not necessarily depict minors engaging in sexually explicit conduct.

d. "Child pornography," as defined in 18 U.S.C. § 2256(8), is any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image of picture, whether made or produced by electronic, mechanical or other means, of sexually explicit conduct, where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

e. "Computer," as used herein, refers to "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device" and includes smartphones, and mobile phones and devices. *See* 18 U.S.C. § 1030(e)(1).

f. "Computer hardware," as used herein, consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes,

and other memory storage devices); peripheral input/output devices (including keyboards, printers, video display monitors, and related communications devices such as cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including physical keys and locks).

g. "Computer passwords and data security devices," as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates what might be termed a digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

h. "Hashtag," as used herein, refers to a word or phrase preceded by a hash or pound sign (#), which is used to identify messages or groups on a specific topic.

i. "Internet Protocol address" or "IP address," as used herein, refers to a unique number used by a computer or other digital device to access the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer or device accessing the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer or device may be directed properly from its source to its destination. Most Internet Service

Providers (ISPs) control a range of IP addresses. IP addresses can be "dynamic," meaning that the ISP assigns a different unique number to a computer or device every time it accesses the Internet. IP addresses might also be "static," if an ISP assigns a user's computer a particular IP address that is used each time the computer accesses the Internet. ISPs typically maintain logs of the subscribers to whom IP addresses are assigned on particular dates and times.

j. "Internet Service Providers" ("ISPs"), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment.

k. The "Internet" is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

l. "Minor," as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.

m. "Mobile applications," as used herein, are small, specialized programs downloaded onto mobile devices that enable users to perform a variety of functions, including engaging in online chat, reading a book, or playing a game.

n. "Records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.

o. "Remote Computing Service" ("RCS"), as defined in 18 U.S.C. § 2711(2), is the provision to the public of computer storage or processing services by means of an electronic communications system.

p. "Sexually explicit conduct," as defined in 18 U.S.C. § 2256(2), means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person.

q. A "storage medium" is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, thumb drives, and other magnetic or optical media.

r. "Visual depiction," as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

PROBABLE CAUSE

6. Canadian law enforcement officers have reported to HSI that on March 22, 2016, an officer with the Saskatchewan Police Service (SPS) in Saskatchewan, Canada, arrested an

individual (hereinafter "John Doe") for parole violations.[1] Pursuant to the arrest, SPS seized John Doe's iPhone. John Doe told SPS that he had been using an online mobile chat application to download and distribute child pornography images and videos to a network of other users of the mobile chat application. He provided SPS his username and login information for the application and gave SPS consent to take over and use his account to conduct investigations and gather evidence. This chat application is hereinafter referred to as "Application A."[2] HSI was not involved with the user's arrest.

7. "Application A" is designed for mobile chatting or messaging. To use this application, a user downloads the application to a mobile phone or other mobile device via a service such as Google Play Store, Apple iTunes, or another similar provider. Once downloaded and installed, the user is prompted to create an account and username. The user also has a display name, which is what other users see when transmitting messages back and forth. Once the user has created an account, the user is able to locate other users via a search feature, and the two parties can then send each other messages, images, and videos.

8. "Application A" users are also able to create chat groups, of up to 50 people, to communicate in a group setting and exchange images and videos. These groups are administered

---

[1] John Doe's true name is known to law enforcement. This investigation remains active and disclosure of Doe's true name would potentially alert investigative suspects to the fact that law enforcement action is being taken, thereby provoking suspects to notify other users of law enforcement action, flee, and/or destroy evidence.

[2] The actual name of "Application A" is known to law enforcement. This chat application remains active and disclosure of the name of the application would potentially alert its users to the fact that law enforcement action is being taken against users of the application, thereby provoking users to notify other users of law enforcement action, flee, and/or destroy evidence. Accordingly, to protect the confidentiality and integrity of the ongoing investigation involved in this matter, specific names and other identifying factors have been replaced with generic terms and the application will be identified herein as "Application A."

by the group creator who has the authority to remove and ban other users from the created group. Once the group is created, "Application A" users have the option of sharing a link to the group that includes all of their contacts or any other user. These groups are frequently created with a "hashtag" that is easily identifiable or searchable by keyword.

9. SPS was able to log in and secure John Doe's "Application A" account. In reviewing the chat conversations held with John Doe's account, SPS was able to identify 72 unique "Application A" users who had shared at least one image or video of child pornography with John Doe directly, or who had posted child pornography in one of the "Application A" groups to which John Doe belonged, and six "Application A" users who had posted a message between or commented on child pornography images or videos. Many of the groups to which John Doe belonged had names that included terms that your affiant knows through training and experience to be suggestive of child pornography.

10. SPS logged all of the information regarding the messages and saved all of the images and videos of child pornography shared with John Doe's account. SPS sent preservation requests to "Application A" regarding all 78 accounts referenced in the previous paragraph between April 20 and April 30, 2016. SPS transmitted to HSI the information logged and saved from the review of John Doe's "Application A" account.

11. On June 28, 2016, a Production Order was issued by a Provincial Court Judge in Saskatchewan, Canada, ordering "Application A" to produce user information and saved content regarding these 78 accounts. On September 15, 2016, SPS received the requested results from "Application A." The information received from "Application A," including the Certification of

Records provided by "Application A," was transmitted to HSI, along with a copy of the Production Order issued by the Provincial Court Judge.

12. The results provided by "Application A" included, among other things, additional images and videos of child pornography recently shared by the 78 accounts. This included both child pornography shared with John Doe and child pornography shared with other individuals and groups not related to John Doe's account. Additional Production Orders were served on "Application A" for information regarding the "Application A" accounts who shared child pornography with the originally investigated 78 accounts, leading to the identification of additional "Application A" accounts beyond the 78 accounts that shared child pornography with John Doe.

13. Your affiant has reviewed the information received from "Application A." A review of that information shows that April 2, 2016 an "Application A" user with the account name "bluegreen19" used "Application A" to share a video of child pornography. Specifically, the video shared by "bluegreen19" included the following:

a. **File name:** 1459568709575-cc4ab178-3a9b-480d-a859-49e40a8b3fd1.mp4

Description: a video, approximately 24 seconds in length, of an adult female inserting a sexual device into a nude prepubescent female's anus.

14. The information provided by "Application A" included IP addresses used by the target account. Specifically, IP address 100.40.20.91 was used by "bluegreen19" on February 25, 2017 at 04:47:17 UTC. A query of the American Registry for Internet Numbers ("ARIN")

online database revealed that IP address 100.40.20.91 was registered to Verizon Internet Services, Inc. ("Verizon").

15. On June 9, 2017, a U.S. Department of Homeland Security summons was issued to Verizon in regard to the IP address described in Paragraph 12. A review of the results obtained on June 23, 2017 identified the following account holder and address, which is the address of the SUBJECT PREMISES:

IP Address:	100.40.20.91
Start time:	2016-08-17 @ 05:08:11Z
Stop time:	2017-04-26 @ 04:32:11Z
Duration:	251d 23h 24min 0s
Customer ID:	154084724
Customer name:	Jonathan Breslin
Account address:	9 Grove Av FLR 3 WSTY, RI 02891
User ID:	vze1el1ow
User Name:	jbreslin710

16. A check of publicly available databases also revealed that Jonathan BRESLIN resides at the SUBJECT PREMISES.

17. A check with the Rhode Island State Police (RISP) Fusion Center on or about July 3, 2017, revealed that an individual named Jonathan BRESLIN with a date of birth of

(XX/XX/1985) has a RI driver's license with a previous address listed. The check also revealed that BRESLIN does not have any vehicles registered in his name.

18. On or about July 11, 2017, representatives of the U.S. Postal Service stated that Jonathan BRESLIN is currently receiving mail at the SUBJECT PREMISES.

19. Surveillance of the SUBJECT PREMISES on or about July 7, 2017 revealed that the number "9" is clearly marked on the front door of the house.

20. A search of a public records database that provides names, dates of birth, addresses, associates, telephone numbers, email addresses, etc., was conducted for Jonathan BRESLIN. These public records indicated that BRESLIN's current address is 9 Grove Avenue, Apartment 3, Westerly, RI 02891. The records also indicated that an email address BRESLIN provided to "Application A" (rainshadow39@gmail.com) is also affiliated with an Amazon account in the name of Jonathan BRESLIN.

21. A check of open source information from the Internet regarding BRESLIN revealed that BRESLIN, using the SUBJECT PREMISES address, filed corporation paperwork in the state of Connecticut on January 17, 2017 for a company named Poquonnock Group, LLC. The website also revealed that the company dissolved in June of 2017.

22. On July 28, 2017, I served an administrative subpoena on Application A for subscriber information for the username "Bluegreen19." On July 31, 2017, Application A responded with updated IP address information for "Bluegreen19." Specifically, IP address 108.34.203.193 was used by "bluegreen19" on July 2, 2017 at 01:11:53 UTC and July 29, 2017 at 13:25:25 UTC. A query of the American Registry for Internet Numbers ("ARIN") online

database revealed that IP address 108.34.203.193 was registered to Verizon Internet Services, Inc. ("Verizon").

23. On July 31, 2017, a U.S. Department of Homeland Security summons was issued to Verizon in regard to the IP address described in Paragraph 22. A review of the results obtained on August 7, 2017 identified the following account holder and address, which is the address of the SUBJECT PREMISES:

IP Address:	108.34.203.193
Customer ID:	154084724
Customer name:	Jonathan Breslin
Account address:	9 Grove Av
	FLR 3
	WSTY, RI 02891
User ID:	vze1el1ow
User Name:	jbreslin710

24. On August 1, 2017, acting in an undercover capacity, your affiant sent an unsolicited "chat" message to the username "Bluegreen19" via "Application A." "Bluegreen19" responded shortly thereafter. The initial unsolicited chat and response are excerpted as follows:

UCA (undercover affiant) – I lost all my good stuff!

BLUEGREEN19 – Mr discreet lol

UCA – You like that? Lol

BLUEGREEN19 – Almost too discreet lol

UCA – My computer crashed and I lost everything

BLUEGREEN19 – Where do I know you from?

UCA – I saved your contact after we talked in a "group" a while back. I only save the ones I trust.

BLUEGREEN19 – Gottttcha

25. "Bluegreen19" provided some technical advice regarding recovering lost data, then the following exchange occurred in which "Bluegreen19" suggested using another social media application, "Application B" to obtain child pornography and child erotica:

UCA – Can you hook a brother up? lol

BLUEGREEN19 – Did u ever check out [Application B]?

BLUEGREEN19 – I panicked and deleted everything lol

UCA – It may have been in my favorites

BLUEGREEN19 – I only have candids of girls eating ice cream next door lol

UCA – Wh did you panic?

BLUEGREEN19 – Gf found out I cheated on her, thought she was gonna DIG through my phone

UCA – Oh shit! That sucks!

BLUEGREEN19 – U don't even know…

UCA – You sent me some good shit a while back! That's why I saved you! Lol

BLUEGREEN19 – [Application B]

BLUEGREEN19 – Get. That. Shit. Lol

26. Application B is a mobile application that provides users a platform to post videos of themselves and share them with friends or the world. Application B also contains a feature which allows the user to stream themselves live. Within Application B, users can post comments to a broadcaster's performance and send "likes" to the performers they enjoy. Users create a

username and password, and can follow other users. Application B's terms of service require that users be at least 13 years old to use the platform and its guidelines state that users should not post sexually explicit or nude videos or images.

27. "Bluegreen19" described viewing videos of children engaged in sexually explicit activity notwithstanding Application B's terms of service:

> UCA – It's an app? What's kind of shit is on there?
>
> BLUEGREEN19 – I got banned for comments..u can't use keywords but those girls do CRAZY shit with HD cams
>
> BLUEGREEN19 – Its supposed to be a sing along lip sync music video thing
>
> BLUEGREEN19 – But girls can go live
>
> UCA – Nice! How old?
>
> BLUEGREEN19 – Younnnggggg lol
>
> UCA – And they do more than sing? Lol
>
> BLUEGREEN19 – Omg yes
>
> BLUEGREEN19 – I watched what had to be an 8yo stick a mini toy bowling pin(the top part) up her ass, pull it out and suck on it
>
> BLUEGREEN19 – Girls in the tub pissing into their mouths
>
> BLUEGREEN19 – So many close up orgasms
>
> BLUEGREEN19 – I really need to get that shit back…
>
> UCA – Can't you just sign up under a different name?
>
> BLUEGREEN19 – Girls TRYING to stick things in their pussies and saying ow
>
> BLUEGREEN19 – Yeah totally
>
> BLUEGREEN19 – I get paranoid and try to stay away but goddamn
>
> BLUEGREEN19 – The shit I've seen

28. Bluegreen19 then stated that he convinced some minor females that he found on Application B to communicate with him on Application A and coerced at least one minor female to engage in sexually explicit activity:

BLUEGREEN19 – Got a few of them to hit me up on [Application A]

BLUEGREEN19 – Oh shit ill give u her name

BLUEGREEN19 – Just share what u get lol

UCA – Absolutely! I'm so hard up for that shit right now!

BLUEGREEN19 – [username redacted by your affiant]

UCA – And how old is she?

BLUEGREEN19 – She won't talk to me anymore lol

UCA – Why?

BLUEGREEN19 – She said 13 but not older than ten

UCA – Wow! And she did the shit you told her to do?

BLUEGREEN19 – She showed her pussy and face in the same pic

BLUEGREEN19 – Sexy fucking glasses

BLUEGREEN19 – Bald n wet

29. Your affiant reviewed the Application B account of the username identified above by "Bluegreen19" and observed a video of a minor female, approximately 8 to 10 years old, lipsyncing a pop song and licking her lips in a sexually suggestive manner.

30. "Bluegreen19" also described showing pornographic material to minors:

BLUEGREEN19 – I showed these 2 little girls a rough gangbang vid and they were like "stop it! They're being mean to the pretty lady!" I had to explain that she likes it

31. Your affiant asked "Bluegreen19" about groups on Application A:

> UCA – Any good [Application A] groups groups lately? Every good one I find is full! So frustrating!
>
> BLUEGREEN19 – Lol
>
> BLUEGREEN19 – I haven't been in one in ages
>
> BLUEGREEN19 – I only have non nude candids
>
> UCA – Well I know you had some good shit back then because like I said I only save the ones I like and trust! Lol

32. At this point, "Bluegreen19" sent me three image of a fully clothed minor female. It appears that the pictures were taken out of the window of a car.

33. "Bluegreen19" subsequently sent a link to a video on Application B. The video is child erotica of a minor female in a bikini dancing in a seductive manner. The girl then turns around and the bathing suit bottom is pulled up into the crack of her bottom. "Bluegreen19" then sent another link to video on Application B of a minor female in underwear or pajamas dancing. The girl's bottoms are pulled up showing the outline of her vagina.

34. On August 4, 2017, "Bluegreen19" sent me a chat via Application A in which he described wanting to molest his girlfriend's 6 or 7 year old niece:

> BLUEGREEN19 – Had a dream last night I was jerking off over my gfs nieces sleeping face, was so real
>
> BLUEGREEN19 – Any headway in [Application B]?
>
> UCA – Not yet. I guess networking takes some time! I tried the hard drive thing to recover my stash and it didn't work

BLUEGREEN19 – There's def ways to recover them, might have to spend some money on recovery software

BLUEGREEN19 – I wish I didn't delete all my shit…

BLUEGREEN19 – Had a ton of vids of little girls getting flashed with big dick, loved the reactions

UCA – Have to build the stash back up lol

BLUEGREEN19 – So paranoid these days lol fuckin sucks

UCA – Things will blow over with the gf

BLUEGREEN19 – I want to get the niece to sleep over fuckin bad lol

BLUEGREEN19 – Want her *

BLUEGREEN19 – It's a loft style apartment so it's one giant room, would be so easy to jerk it right over her sleeping face and cum on her pillow

BLUEGREEN19 – After my gf falls asleep of course

BLUEGREEN19 – I thought maybe I could cum on her lips and could say she was drooling if she woke up…But that's risky business lol

UCA – Especially if the gf is sleeping in the same room!

BLUEGREEN19 – Fuck yes!

BLUEGREEN19 – I want her to fall asleep on my lap so I can rub my dick on her little mouth without a lot of moving around

BLUEGREEN19 – Trying to have a star wars night with her (so the gf leaves)

UCA – How old?

BLUEGREEN19 – I'd go in the next room and shoot the biggest load into a bowl of ice cream and cover it with chocolate syrup and whipped cream and only put one small scoop so when she asks for more I can tell her to lick the bowl clean first

BLUEGREEN19 –6or7now

BLUEGREEN19 – What would you do?

UCA – I think you are braver than I am lol

BLUEGREEN19 – Lol

BLUEGREEN19 – It would be hot if she was just pretending to sleep

UCA – You think she'd sleep thru it?

BLUEGREEN19 – My gf?

BLUEGREEN19 – Or getting cum shot on her lips?

35. "Bluegreen19" then described possibly drugging the minor female in order to molest her:

BLUEGREEN19 – I'd like to get her tuckered out from playing in the snow or something, maybe crush up a tylenol pm on that ice cream or something

BLUEGREEN19 – Some kids when they pass out u can pick them up and put them in bed and they are OUT

BLUEGREEN19 – I think you'd have a shot of they were that out

UCA – Have you ever done anything like that before? So hot!

BLUEGREEN19 – I haven't but I think about it all the time lol

36. At this point, "bluegreen19" sends a link to a video on Application B. The video is of a minor female in a bikini dancing on what appears to be beach. The girl pulls on the bikini top and the bikini bottoms show the outline of her vagina.

37. In addition, "Bluegreen19" a link to a video of post-pubescent pornography on Application B, specifically a close up video of a post-pubescent female urinating. It is unclear whether the video is of an adult or a post-pubescent minor.

38. On August 8, 2017, "Bluegreen19" sent me a "chat" message via Application A in which he again referred to possible molesting his girlfriend's niece:

BLUEGREEN19: Lol I gotta bring up movie night without sounding fucking weird

UCA: Your gf would think its weird if you wanted to do a movie night?

BLUEGREEN19: No either she or the kid brought it up already, just gotta figure out how to work it out without being weird

BLUEGREEN19: Maybe I can take her swimming and get her to take a shower after

39. At this point, "Bluegreen19" sent me a link to a video on Application B featuring a minor female, approximately 7 or 8 years old years old, wearing a bikini top and panty underwear, dancing.

BLUEGREEN19: This girls fuckin body…i just wanna bury my face in that ass

BLUEGREEN19: I would drug the shit out of that girl if I had half a chance

BACKGROUND ON CHILD PORNOGRAPHY, COMPUTERS, AND THE INTERNET

40. I have had both training and experience in the investigation of computer-related crimes. Based on my training, experience, and knowledge, I know the following:

a. Computers and digital technology are the primary way in which individuals interested in child pornography interact with each other. Computers basically serve four functions in connection with child pornography: production, communication, distribution, and storage.

b. Digital cameras and smartphones with cameras save photographs or videos as a digital file that can be directly transferred to a computer by connecting the camera or smartphone to the computer, using a cable or via wireless connections such as "WiFi" or "Bluetooth." Photos and videos taken on a digital camera or smartphone may be stored on a removable memory card in the camera or smartphone. These memory cards are often large enough to store thousands of high-resolution photographs or videos.

c. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Mobile devices such as smartphones and tablet computers may also connect to other computers via wireless connections. Electronic contact can be made to literally millions of computers around the world. Child pornography can therefore be easily, inexpensively and anonymously (through electronic communications) produced, distributed, and received by anyone with access to a computer or smartphone.

d. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. Electronic storage media of various

types – to include computer hard drives, external hard drives, CDs, DVDs, and "thumb," "jump," or "flash" drives, which are very small devices which are plugged into a port on the computer – can store thousands of images or videos at very high resolution. It is extremely easy for an individual to take a photo or a video with a digital camera or camera-bearing smartphone, upload that photo or video to a computer, and then copy it (or any other files on the computer) to any one of those media storage devices. Some media storage devices can easily be concealed and carried on an individual's person. Smartphones and/or mobile phones are also often carried on an individual's person.

e. The Internet affords individuals several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

f. Individuals also use online resources to retrieve and store child pornography. Some online services allow a user to set up an account with a remote computing service that may provide e-mail services and/or electronic storage of computer files in any variety of formats. A user can set up an online storage account (sometimes referred to as "cloud" storage) from any computer or smartphone with access to the Internet. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer, smartphone or external media in most cases.

g. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional (*i.e.*, by saving an e-mail as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files).

Digital information can also be retained unintentionally such as the traces of the path of an electronic communication may be automatically stored in many places (*e.g.*, temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

41. As described above and in Attachment B, this application seeks permission to search for records that might be found at the SUBJECT PREMISES, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

42. I submit that if a computer or storage medium, including a smart phone, is found at the SUBJECT PREMISES, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file

on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

43. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the

purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium at the SUBJECT PREMISES because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information,

communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs,

may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

f. I know that when an individual uses a computer to obtain or access child pornography, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

44. Based upon my training and experience and information relayed to me by agents and others involved in the forensic examination of computers, I know that computer data can be stored on a variety of systems and storage devices, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact disks, magnetic tapes, memory cards,

memory chips, and online or offsite storage servers maintained by corporations, including but not limited to "cloud" storage. I also know that during the search of the premises it is not always possible to search computer equipment and storage devices for data for a number of reasons, including the following:

a. Searching computer systems is a highly technical process which requires specific expertise and specialized equipment. There are so many types of computer hardware and software in use today that it is impossible to bring to the search site all of the technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may also be necessary to consult with computer personnel who have specific expertise in the type of computer, software website, or operating system that is being searched;

b. Searching computer systems requires the use of precise, scientific procedures which are designed to maintain the integrity of the evidence and to recover "hidden," erased, compressed, encrypted, or password-protected data. Computer hardware and storage devices may contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Since computer data is particularly vulnerable to inadvertent or intentional modification or destruction, a controlled environment, such as a law enforcement laboratory, is essential to conducting a complete and accurate analysis of the equipment and storage devices from which the data will be extracted;

c. The volume of data stored on many computer systems and storage devices will typically be so large that it will be highly impractical to search for data during the execution of the physical search of the premises; and

d. Computer users can attempt to conceal data within computer equipment and storage devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension ".jpg" often are image files; however, a user can easily change the extension to ".txt" to conceal the image and make it appear that the file contains text. Computer users can also attempt to conceal data by using encryption, which means that a password or device, such as a "dongle" or "keycard," is necessary to decrypt the data into readable form. In addition, computer users can conceal data within another seemingly unrelated and innocuous file in a process called "steganography." For example, by using steganography a computer user can conceal text in an image file which cannot be viewed when the image file is opened. Therefore, a substantial amount of time is necessary to extract and sort through data that is concealed or encrypted to determine whether it is contraband, evidence, fruits, or instrumentalities of a crime.

45. Additionally, based upon my training and experience and information related to me by agents and others involved in the forensic examination of computers, I know that routers, modems, and network equipment used to connect computers to the Internet often provide valuable evidence of, and are instrumentalities of, a crime. This is equally true of so-called "wireless routers," which create localized networks that allow individuals to connect to the Internet wirelessly. Though wireless networks may be "secured" (in that they require an

individual to enter an alphanumeric key or password before gaining access to the network) or "unsecured" (in that an individual may access the wireless network without a key or password), wireless routers for both secured and unsecured wireless networks may yield significant evidence of, or serve as instrumentalities of, a crime—including, for example, serving as the instrument through which the perpetrator of the Internet-based crime connected to the Internet and, potentially, containing logging information regarding the time and date of a perpetrator's network activity as well as identifying information for the specific device(s) the perpetrator used to access the network. Moreover, I know that individuals who have set up either a secured or unsecured wireless network in their residence are often among the primary users of that wireless network.

46. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

CHARACTERISTICS COMMON TO INDIVIDUALS WHO ADVERTISE, TRANSPORT, DISTRIBUTE, RECEIVE, POSSESS, AND/OR ACCESS WITH INTENT TO VIEW CHILD PORNOGRAPHY

47. Based on my previous investigative experience related to child exploitation investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know there are certain characteristics common to individuals who distribute, receive, possess, and/or access with intent to view child pornography:

a. Such individuals may receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media, or from literature describing such activity.

b. Such individuals may collect sexually explicit or suggestive materials in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Such individuals almost always possess and maintain their hard copies of child pornographic material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. Individuals who have a sexual interest in children or images of children typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years.

d. As noted above, when your affiant, in an undercover capacity, asked "Bluegreen19" if he could "hook a brother up" (i.e., share child pornography), "Bluegreen19" stated that he "panicked and deleted everything" because his "Gf found out I cheated on her, thought she was gonna DIG through my phone." Based on my

training and experience, it is typical of individuals involved in child pornography to be initially reluctant to admit possessing child pornography or be willing to share such materials with other individuals on-line and to falsely and or inaccurately claim they deleted "all" of their child pornography collections. Often times such individuals maintain child pornography on a variety of different media and continue to keep child pornography even when some such materials are "deleted". This is particularly true of individuals, such as "Bluegreen19" who have distributed child pornography in the past.

e. Likewise, such individuals often maintain their child pornography images in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These child pornography images are often maintained for several years and are kept close by, usually at the possessor's residence, inside the possessor's vehicle, or, at times, on their person, to enable the individual to view the child pornography images, which are valued highly. Some of these individuals also have been found to download, view, and then delete child pornography on their computers or digital devices on a cyclical and repetitive basis.

f. Importantly, evidence of such activity, including deleted child pornography, often can be located on these individuals' computers and digital devices through the use of forensic tools. Indeed, the very nature of electronic storage means that evidence of the crime is often still discoverable for extended periods of time even after the individual "deleted" it.[3]

[3] *See United States v. Carroll*, 750 F.3d 700, 706 (7th Cir. 2014) (concluding that 5-year delay was not too long because "staleness inquiry must be grounded in an understanding of both the behavior of child pornography collectors

g. Such individuals also may correspond with and/or meet others to share information and materials, rarely destroy correspondence from other child pornography distributors/possessors, conceal such correspondence as they do their sexually explicit material, and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

h. Such individuals prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world. Thus, even if BRESLIN uses a portable device (such as a mobile phone) to access the internet and child pornography, it is more likely than not that evidence of this access will be found in his home, the SUBJECT PREMISES, as set forth in Attachment A.

REQUEST FOR SEALING OF WEBSITE/AFFIDAVIT

48. It is respectfully requested that this Court issue an order sealing, until further order of this Court, all papers submitted in support of this Application, including the Application, Affidavit, and Search Warrant, and the requisite inventory notice (with the exception of one copy of the warrant and the inventory notice that will be left at the SUBJECT PREMISES). Sealing is necessary because the items and information to be seized are relevant to an ongoing investigation and not all of the targets of this investigation will be searched at this time. Based upon my

---

and of modern technology"); *see also United States v. Seiver*, 692 F.3d 774 (7th Cir. 2012) (Posner, J.) (collecting cases, e.g., *United States v. Allen*, 625 F.3d 830, 843 (5th Cir. 2010); *United States v. Richardson*, 607 F.3d 357, 370–71 (4th Cir. 2010); *United States v. Lewis*, 605 F.3d 395, 402 (6th Cir. 2010).)

training and experience, I have learned that online criminals actively search for criminal affidavits and search warrants via the Internet, and disseminate them to other online criminals as they deem appropriate, *i.e.*, post them publicly online through forums. Premature disclosure of the contents of this Affidavit and related documents may have a significant and negative impact on this continuing investigation and may jeopardize its effectiveness by alerting potential targets to the existence and nature of the investigation, thereby giving them an opportunity to flee, or to destroy or tamper with evidence.

CONCLUSION

49. Based on the foregoing, there is probable cause to believe that the federal criminal statutes cited herein have been violated, and that the contraband, property, evidence, fruits and instrumentalities of these offenses, more fully described in Attachment B, are located at the locations described in Attachment A. I respectfully request that this Court issue a search warrant for the locations described in Attachment A, authorizing the seizure and search of the items described in Attachment B.

50. I am aware that the recovery of data by a computer forensic analyst takes significant time; much the way recovery of narcotics must later be forensically evaluated in a lab, digital evidence will also undergo a similar process. For this reason, the "return" inventory will contain a list of only the tangible items recovered from the premises. Unless otherwise ordered by the Court, the return will not include evidence later examined by a forensic analyst.

James V. Richardson
Special Agent
Homeland Security Investigations

Sworn and subscribed before me this 8 day of August, 2017.

HON. PATRICIA A. SULLIVAN
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

DESCRIPTION OF LOCATIONS TO BE SEARCHED

The entire property located at 9 Grove Avenue, Floor 3, Westerly, RI 02891, including the residential building, any outbuildings, and any appurtenances thereto (the SUBJECT PREMISES). The building is a three family, two and a half story building with yellow vinyl siding and white and green trim. The number "9" is clearly affixed to the front door of the building.

ATTACHMENT B

ITEMS TO BE SEIZED

The following materials, which constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use or which is or has been used as the means of committing a criminal offense, namely violations of Title 18, United States Code, Sections 2252, 2252A and 2422:

1. Computers or storage media, including smart phones, used as a means to commit the violations described above.
2. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):
    a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
    b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
    c. evidence of the lack of such malicious software;

d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to the crime(s) under investigation and to the computer user;

e. evidence indicating the computer user's knowledge and/or intent as it relates to the crime(s) under investigation;

f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

g. evidence of programs (and associated data) that are designed to eliminate data from the COMPUTER;

h. evidence of the times the COMPUTER was used;

i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

k. records of or information about Internet Protocol addresses used by the COMPUTER;

l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses; and

m. contextual information necessary to understand the evidence described in this attachment.

3. Routers, modems, and network equipment used to connect computers to the Internet.
4. Child pornography and child erotica.
5. Records, information, and items relating to violations of the statutes described above including:
    a. Records, information, and items relating to the occupancy or ownership of the SUBJECT PREMISES, 9 Grove Avenue, Floor 3, Westerly, RI 02891, including utility and telephone bills, mail envelopes, or addressed correspondence;
    b. Records, information, and items relating to the ownership or use of computer equipment found in the above residence, including sales receipts, bills for Internet access, and handwritten notes;
    c. Records and information relating to the identity or location of the persons suspected of violating the statutes described above;
    d. Records and information relating to the sexual exploitation of children, including correspondence and communications between users of "Application A" and "Application B";
    e. Records and information showing access to and/or use of "Application A" and "Application B"; and
    f. Records and information relating or pertaining to the identity of the person or persons using or associated with the "Application A" user "bluegreen19".

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing

or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact discs, magnetic tapes, memory cards, memory chips, and other magnetic or optical media.